ISSN: 2454-2415 Vol. 6, Issue 5, 2018 May, 2018 DOI 11.25835/IJIK-50 www.doie.org

Cryptography for Online Security: Applications of Number Theory

Chetna
Faculty, PG Department of Mathematics,
M.M. Modi College, Patiala, Punjab, India.
Cell No: +91-9501377088

ABSTRACT
Over the years the rate at which sensitive information is sent through the internet has increased radically and as a result cyber criminals are taking serious interest in the ways and means to compromise e-channels. Number theory one of the major branches of mathematics provide theoretical results that have many crucial applications in the security of coded information. This branch of specialised knowledge provides the basis for information security known as 'Cryptography' that is encrypting the data for confidentiality. This paper gives the brief overview of the results from number theory which play an important role in the online security. The paper also highlights how these results can be used to secure information.

INTRODUCTION

With e-banking channels being used intensively by an increasing number of people everyday, cyber criminals are taking serious interest in the ways and means to compromise e-channels. Advanced tech based attack methods now attempt to trick out the username and password. Even a better, but still basic method as two-factor authentication seems insufficient now. The reason is that hackers have found ways to entice users to enter access codes through fake user interfaces of payment sites. Similarly, online businesses face various threats in their daily business, with the main concern being the online business and the online security of the company. The online world is full of such security risks, ranging from hackers to brute force attacks. One of the biggest online threats is Distributed Denial of Service (DDoS) attacks. In short, they mean that a large network of infected computers will try to connect to a website in large numbers in order to overload the server, which will cause a website to slow down considerably, become unavailable or even this way important sensitive confidential data can be lost. This means it is not only a direct loss due to lost revenue, but also additional costs to solve the problem and to recover lost data. The often gigantic databases of persons and of financial nature makes online business companies an ideal target for cyber-attacks. Hybrid cloud environments are nowadays are the norm rather than the exception in today's business world. But with data and processes fragmented across multiple clouds, the chances of a leak or hack increases without measures. Thus, due to computational capability a computer can quickly break the coded messages. And in the modern world where the electronic communication occupies a fundamental place, security of information is at huge risk. But the question is how we can best address these challenges? Now, here comes the role of mathematics into play. Number theory one of the major branches of mathematics provide theoretical results that have many crucial applications in the security of coded information. This branch of specialised knowledge for information security is known as 'Cryptography' that is encrypting the data for confidentiality. Cryptography can also be used for another applications – digital signature, currently one of the most important methods to ensure soundness. For the latter application is not only an important technique of cryptography, but also an organizational measure of a Certification Provider (CA). The latter appears as a Trusted Third Party (TTP) stamp which is common figure frequently seen in the software contents. The number theory addresses these security problems through RSA Cryptosystem, Diffie-Hellman key distribution method, simple encryption, Hill Cipher technique and many more. This paper gives the brief overview of the results from number theory which play an important role in the online security. The paper also highlights how these results can be used to secure information.

To understand how these algorithms works, we shall need some mathematical results from Number Theory [3]. The objective of this paper is to highlight the significance of these important results from number theory which further help us in making secure the information exchange during online transactions.

CRYPTOGRAPHY

Cryptography can be described as the art of hidden writing. In the older days, this was done by hiding the text itself or replacing it with secret symbols, but nowadays mathematical techniques have enriched this area. A text can be created using a cryptographic algorithm and a key (the source text) are transformed into an unreadable slush characters (the code text). The receiver must reset the

algorithm and a key to get the source text back. There are two types of cryptography:

Secret-key cryptography in which transmitter and the receiver use the same key.

Public-key cryptography uses two different keys – one key (public key) may be known to everyone, the other (secret key) is only known to the recipient. With the public key the sender can send the code text, and the recipient can use the secret key to recover the source text. Normally, the sender and the recipient of a message use the same key, for which they agree together in advance. They can then use secret key to encrypt and decrypt the message. That is not, however always practical, for example over a network they may not know each other. In such a case, public key cryptography is useful. The receiver creates two keys, a public and a secret. The first he can publish anywhere (for example on his homepage or in a public space), so that anyone who wants to send him a message can retrieve it. He must keep the second key secret. Messages that others will send will be encrypted through his public key, only he can use his secret key to translate back the source text. To encrypt something you always need an algorithm. This is the way through which information is changed (coded). Algorithms can be very simple or very complex. Even the small children sometimes create an algorithm when they certain words as 'secret code'. Here you count one with each letter, so that an unreadable word is created. Of course, in professional cryptography more complicated algorithms are used. The most important algorithms can be divided into two categories:

Public Key Cryptosystems (Asymmetric Cryptosystems): This form of cryptography was invented during the 1970s. This is used as a public key for encryption and a secret key for decoding. An example of Public Key Cryptosystems is the RSA security algorithm. It uses mathematical primes, logarithms and multiplications.

Symmetrical Cryptosystems: In this form of cryptography, there is only one key: the secret key. This key is used for encoding and also for decoding (or in any case, the decoding key can easily be derived from the coding key). The major disadvantage of this is that the key of the transmitter must be passed on to the recipient. In this case, interception of the message prevents communication flow, as a result of which the level of security reduces.

PRIME NUMBERS

Prime numbers are the backbone of cryptography. A prime number is a number which is only divisible by one and the number itself. Thus, an integer $p > 1$ is known as prime number if its only factors are 1 and the number itself. An integer greater than one which is not a prime is known as composite. Prime numbers are very powerful tool which help in securing the information while transferring the data. Billions of money in different currencies crosses the Internet every day but all this e-commerce would not be safe without prime numbers. Even there is prize money worth millions to find out the largest prime number. Presently by [4] the largest prime number known is $2^{43112609} - 1$.

We can understand the usefulness of prime numbers by taking the simple example of credit card security. Let there be two prime numbers p_1 *and* p_2 and when we multiply them, we get the composite number and this composite number is used to generate the public key. This public key is used by the bank to crypt our credit card and keep it safe. Then the prime factors of composite number are used to generate the personal key commonly used to transact through card. The important thing in this process is that when computer combines more and more prime numbers to form the composite numbers and then it becomes impossible for anyone to crack these prime numbers. Prime numbers are unique in nature and thus their knowledge is very important for safe transactions [3].

Further, the concept of Modular Arithmetic together with prime numbers help to share the secret among two people without the interference of third party. In the late 1970s, Diffie-Hellman introduced the method of key exchange based on Modular Arithmetic to solve the key-distribution problem [6]. This allows any two persons to publically transfer data and enables them to share the secret key without anyone's knowledge. When any person would like to share the secret information with another person then many kind of questions arise in their minds as both of them would like to assure the transaction is safe and secure. The first person or the sender would like to assure that only second person or the intended receiver has received the information. Secondly, no third party or anyone else has seen the message. And finally, the receiver would like to be assured that the message has genuinely come from the first person only. All these can be addressed with the help of Modular Arithmetic. The fundamental definition in studying the concept of modular arithmetic establishes a relationship between a pair of integers according to some integer 'm' known as modulus. Technically we can say that:

two integers a and b are congruent modulo m if they differ by an integer multiple of $m, i.e., b - a = km$ for some $k \in Z$. Symbolically it can written as

$$a \equiv b(mod\ m)$$

In other words, $a \equiv b(mod\ m)$ if and only if m divides $a - b$.

If the number we are dividing by is relatively prime to the modulus, then this division leads to unique values. Consequently, if the modulus is a prime then all divisions result in unique values which further are used by the cryptographer. Following properties of modular arithmetic are helpful for a cryptographer to create more and more unique values to create codes [1].

(1) For the integers a and m, reflexivity holds i.e $a \equiv a\ (mod\ m)$.
(2) For the integers $a, b, and\ m$, symmetry holds i.e if $a \equiv b\ (mod\ m)$, then $b \equiv a\ (mod\ m)$.
(3) For the integers $a, b, c, and\ m$, transitivity holds i.e if $a \equiv b\ (mod\ m)$ and $b \equiv c\ (mod\ m)$, then $a \equiv c\ (mod\ m)$.
(4) For the integers $a, b, c, d, and\ m$ under addition if $a \equiv c\ (mod\ m)$ and $b \equiv d\ (mod\ m)$, then $a + b \equiv c + d\ (mod\ m)$.
(5) For the integers $a, b, c, d, and\ m$ under multiplication if $a \equiv c\ (mod\ m)$ and $b \equiv d\ (mod\ m)$, then $ab \equiv cd\ (mod\ m)$.

Modular arithmetic and its properties have been in vogue for hundreds of years. For simple encryption, the following steps are used:

(1) the message is converted into their corresponding numerals.
(2) an invertible modular function is applied to each numeral.
(3) the numerals are reconverted into alphabets.

In this method if we do not use mod function then the decoding of the original message becomes quite simple [2]. But mod function is proven to be an important tool for online security. The mod function is also used to code messages in the technique of Hill Cipher and also in RSA Algorithm. Further, another important tool provided by number theory is Fermat's little theorem and Euler's theorem.

Fermat's little theorem [5]: If p is any prime number and $a \in N, g.c.d(a, p) = 1$ then

$$a^p \equiv a\ mod(p)$$

In other words, $a^p - a$ is an integer multiple of p.

This theorem is very useful in public key and primality test. If we want to check whether the number p is prime or not then consider any natural number co-prime with p. Put all the values in the above equality. If equality holds then p is prime. This theorem is generalised by Euler's for all integers and gives another key to provide online security.

Euler's Totient Theorem [5]: If p is any prime number and a, p are co-primes with the condition that $a < p$, then

$$a^{\varphi(n)} \equiv 1(mod\ n)$$

here $\varphi(n)$ is Totient function. Particularly if $n = p, then\ \varphi(p) = p - 1$.
Fermat's theorem and Euler's theorem use modular arithmetic which provides the ground for strong encryption. In both the cases, in order to build a personal key, a suitable value is required. Let us suppose that the suitable value is represented by a variable say X. Select any two large primes say Y and Z and then multiply them. Then it implies that:

$$\varphi(X) = (Y - 1)(Z - 1)$$

This process will help the bankers to have an appropriate value which is not factored easily and it takes long time to find them. Another way is that we can also consider the variables A and B, where A is relatively prime to $\varphi(X)$. The value of B is calculated from the inverse of $A(mod\varphi(X))$. Then $A\ and\varphi(X)$ are used to create the public key and $B\ and\varphi(X)$ are used to create a private key. This leads to

$$AB \equiv 1(mod\varphi(X)$$

With the use of modular arithmetic, the encryption of the message becomes so secure that it is very difficult for anyone to decode the information without having an idea of the public key. According to these theorems the larger the value of prime number longer it takes to factor their product. Thus, the strength of cryptography actually lies in the application of number theory.

CONCLUSION

Number theory one of the major branches of mathematics provide theoretical results that have many crucial applications in the security of coded information. The paper highlights the application of number theory in the area of cryptography.

Cryptography based on number theory algorithms helps in securing and preserving the data. Cryptography allows the transfer of information in a secure form, ensuring the security, confidentiality and integrity of the data. When protecting confidential information, cryptography contributes to the high level of security of important data of individuals and corporates.

REFERENCES:

[1] Burton David M., *Elementary Number Theory*, 6th Ed., Tata McGraw-Hill, 2010.
[2] D. Stinson, *Cryptography, Theory and Practice*, CRC Press Inc, 2005.
[3] Gerstein Larry; Basic Quadratic Forms, Graduate Studies in Mathematics, Volume 90, American Mathematical Society, (2008).
[4] James S. Kraft and Lawrence C. Washington, *An Introduction to Number Theory with Cryptography*, CRC Press Inc, 2013.

[5] Niven, Zuckerman and Montgomery, *An Introduction to the Theory of Numbers*, 5th Ed., Wiley India Pvt. Ltd., 2010.
[6] W. Diffie and M. E. Hellman., New Directions in Cryptography. IEEE Transactions on Information Theory, IT–22(6):644–654, November 1976.